QS-R-001
REVISION E
EFFECTIVE DATE: April 7,2003

ORGANIZATIONAL ISSUANCE

FAILURE MODE AND EFFECTS ANALYSIS AND CRITICAL ITEMS LIST

OPR(s)	OPR DESIGNEE
QS10, QS20, QS30, and QS40	Robert Fuerst

DOCUMENT HISTORY LOG

Status (Baseline/ Revision/ Canceled)	Document Revision	Effective Date	Description
Baseline		11/20/97	
Revision	A	12/9/97	Remove the word "Groundrules" from Paragraph 8.,Quality Records.
Revision	B	2/9/99	Removed CR5320.3 and CR5320.9 from Applicable Documents, replaced all references of CR5320.9 with Appendix A, and added Appendix A.
Revision	C	7/1/99	Changes made to reflect new organization code changes and/or changes made to reflect new directives renumbering scheme.
Administrative	N/A	8/28/00	OPR and/or OPR Designee change due to personnel transfer or other administrative reason. No other change to the document has been made.
Revision	D	9/09/02	Format and numbering change to implement requirements of QS-A-001 rev F.
Revision	E	04/07/03	OPR and/or OPR Designee change due to personnel transfer or other administrative reason. No other change to the document has been made

Failure Mode and Effects Analysis and Critical Items List

1. SCOPE

1.1 Scope

This Organizational Issuance (OI)is applicable to preparation of Marshall Space Flight Center (MSFC) Failure Mode and Effects Analysis (FMEA) and Critical Items List (CIL) for design, development, and operation phases of all flight hardware and Ground Support Equipment (GSE). This OI also provides evaluation guidelines for reviewing and approving FMEA/CIL.

1.2 Purpose

The purpose of this OI is to provide procedures that shall be used in the performance, evaluation, and approval of FMEA/CIL.

1.3 Applicability

This OI is applicable to all MSFC projects that require FMEA/CIL. The FMEA/CIL groundrules identified in this OI shall be used for performing, reviewing, and approving FMEA/CIL.

2. Applicable Documents

NSTS 22206	*Requirements For Preparation And Approval Of Failure Mode And Effects Analysis (FMEA) And Critical Items List (CIL)*
SSP 30234	*Instructions For Preparation of Failure Modes and Effects Analysis and Critical Items List For Space Station*

3. Definitions

None.

4. Instructions

4.1 Performing FMEA/CIL Analysis

The FMEA/CIL may be performed by either of two methods: (1) functions or (2) hardware The requiurements as specified in the NSTS 22206 or SSP 30234 may be utilized for both approaches. It is also acceptable for the program/project to specify an approach in conducting this analysis.

A functional FMEA/CIL is normally performed early in the design definition phase. This type of analysis is easier to perform for some components by dividing the component into functions and then analyzing each function separately. This method is usually the better method to use for electrical components.

A hardware FMEA/CIL is normally performed after the design has matured past the definition phase. In the hardware method, the component is divided into lower sub-assemblies, modules, and piece parts, and then each is analyzed separately. This type of analysis is usually the better method to use for mechanical, and electromechanical components.

In the process of conducting a FMEA/CIL each item is analyzed for each possible failure mode and for the "worst case" effect. The analysis begins with defining the system, function, and its performance requirements. Assumptions and groundrules to be used in the analysis are specified. Block diagrams are constructed to identify each component analyzed in the FMEA/CIL.

After the method of analysis has been determined and the system has been defined, refer to the applicable FMEA/CIL groundrules (i.e., NSTS 22206, SSP 30234, or Appendix A) for complete analysis instructions.

4.2 **FMEA/CIL Evaluation**

FMEA/CIL analyses shall be reviewed for compliance with the applicable groundrules identified in this OWI.

4.3 **FMEA/CIL Approval**

FMEA/CIL analyses shall be approved in accordance with project requirements.

5. Notes

The Safety and Mission Assurance (S&MA) Office will coordinate the selection and tailoring of the groundrules listed in this OWI, with the program office. Tailoring of the groundrules will be performed on projects other than Shuttle, Space Station, Payloads, and Spacelab.

5.1 **Directive Replacement**. This Directive replaces S&MA-CR10-R-Y-001, Failure Mode and Effects Analysis and Critical Items List.

6. Safety Precautions and Warning Notes

None

7. Appendices, Data, Reports, and Forms

Design information required for performing the FMEA/CIL analysis shall be obtained from design engineers, engineering drawings, project specifications, and other applicable project documentation. Appendix A, found in this OI, may be used to perform, review, and approve future Payload projects/designs. (see Appendix A)

8. **Quality Records**

Quality Record	Repository	Period of Time
FMEA/CIL	As specified by the project plan.	As specified by the project plan.

9. **Tools, Equipment, And Materials**

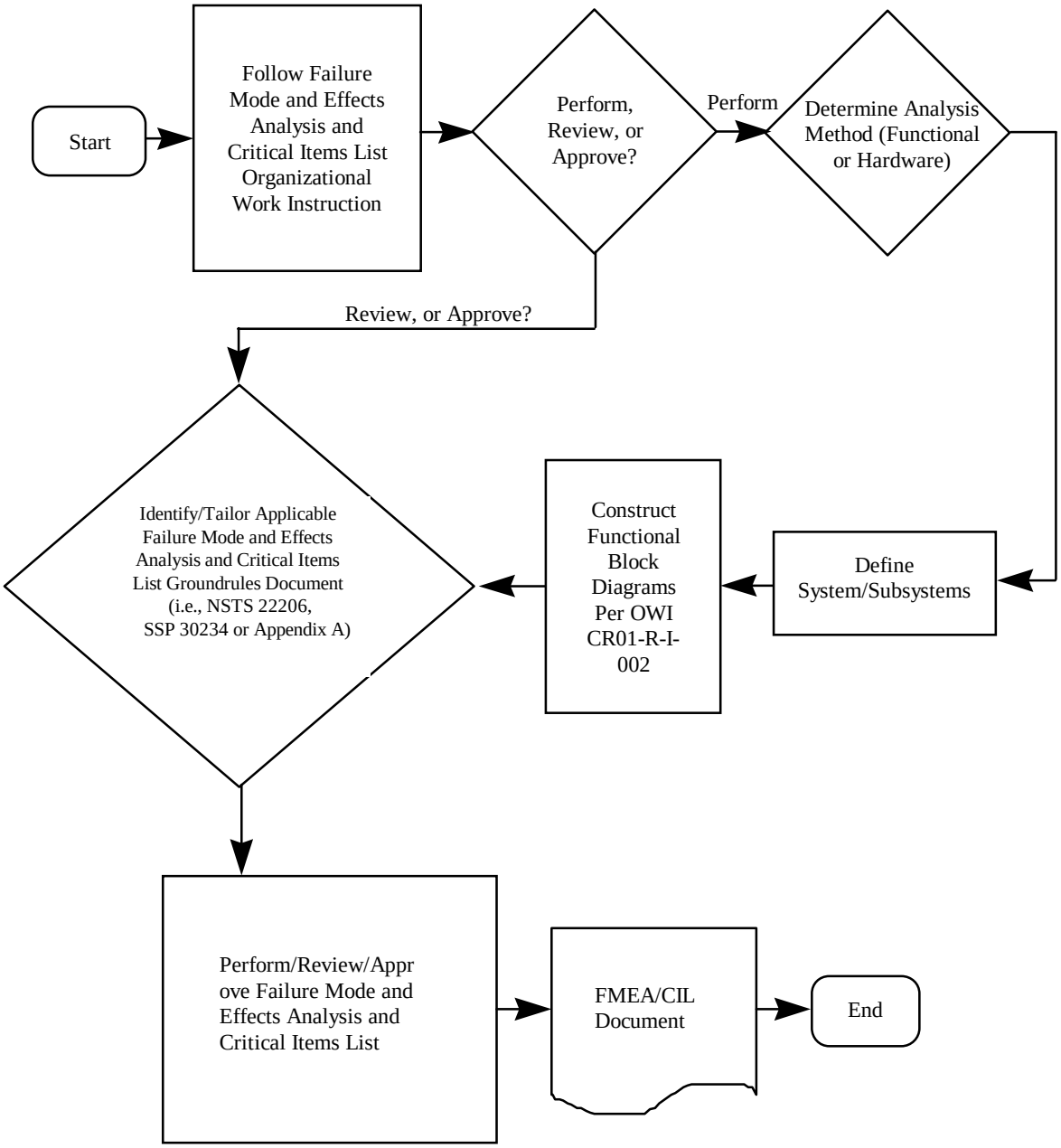
None

10. **Personnel Training And Certification**

FMEA/CIL Preparation training.

11. **Flow Diagram**

The following flow diagram shown on the next page, indicates the sequence of operations to be followed when preparing, reviewing, or approving a FMEA/CIL.


Start
Follow Failure Mode and Effects Analysis and Critical Items List Organizational Work Instruction
Perform, Review, or Approve?
Perform
Determine Analysis Method (Functional or Hardware)
Review, or Approve?
Identify/Tailor Applicable Failure Mode and Effects Analysis and Critical Items List Groundrules Document (i.e., NSTS 22206, SSP 30234 or Appendix A)
Construct Functional Block Diagrams Per OWI CR01-R-I-002
Define System/Subsystems
Perform/Review/Approve Failure Mode and Effects Analysis and Critical Items List
FMEA/CIL Document
End

APPENDIX A

PAYLOAD AND EXPERIMENT

FAILURE MODE AND EFFECTS ANALYSIS

AND CRITICAL ITEMS LIST

CONTENTS

LIST OF FIGURES

ACRONYMS

CIL	Critical Items List
EVA	Extra-Vehicular Activity
FMEA	Failure Mode and Effects Analysis
GFE	Government Furnished Equipment
GSE	Ground Support Equipment
MSFC	Marshall Space Flight Center
NASA	National Aeronautics and Space Administration
NHB	NASA Handbook
OMRSD	Operations and Maintenance Requirements and Specifications Document
OMV	Orbital Maneuvering Vehicle
SFP	Single Failure Point
STS	Space Transportation System
TPS	Thermal Protection System
UCR	Unsatisfactory Condition Report

INTRODUCTION

The enclosed Failure Mode and Effects Analysis (FMEA) and Critical Items List (CIL) groundrules have been developed for use in the design analysis evaluation and certification/ recertification of hardware and software/firmware for Marshall Space Flight Center (MSFC) managed payloads and experiments.

Deviations and changes to these groundrules are not allowed unless approved by the Safety and Mission Assurance Office and the Manager of the Project Office of the payload or experiment under consideration. SCOPE

These groundrules are applicable to MSFC managed payloads/experiments, which meet the criteria shown in section VII of this document, including in-house and out-of-house designs. Any existing payloads/experiments, for which an FMEA/CIL is already required, shall be reanalyzed to be consistent with the requirements contained herein. The reanalysis shall cover criticality categories 1 through 2R as defined in this document. Any deviation from this reanalysis requirement shall be approved by the Safety and Mission Assurance Office and the Project Manager.

MSFC PAYLOAD AND EXPERIMENT FMEA AND CIL GROUNDRULES

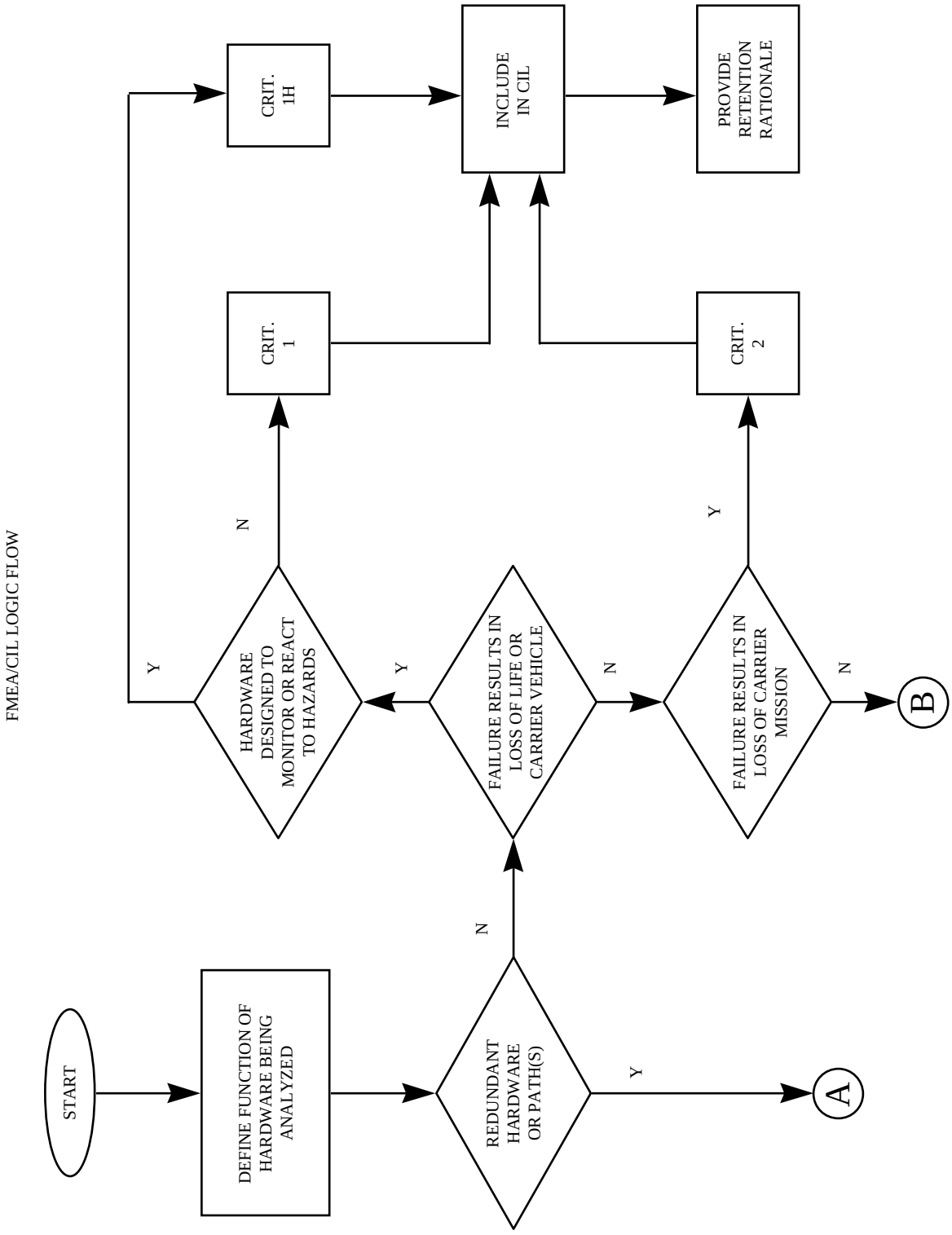
I. FAILURE MODE AND EFFECT ANALYSIS (FMEA)

A. FMEA Content - The FMEA shall analyze all items in the entire design (except as defined in section III, and paragraph VII.B) of the particular payload/experiment, and the design shall reflect the actual flight configuration. The analysis shall also include any ground support equipment (of the given payload/experiment) which is used on criticality category 1, 1R, 1H, 1HR, 2, and 2R hardware during the launch countdown. Any and all interfaces between the given payload/experiment (plus its GSE) and any other flight hardware (carrier or any other payload/experiment) shall be addressed from the standpoint of failure modes and effects propagating across those interfaces. Figure 1 shows the logic flow for the FMEA/CIL analysis.

B. Mission Phases - Effects of failure modes shall be determined and documented for each phase of the payload/experiment mission. The analysis shall begin with the prelaunch integration/ checkout. Subsequent mission phases shall address ascent phase, predeployment operations, deployment, orbital operations, retrieval, stowage, and earth return as appropriate. (See IV for details.)

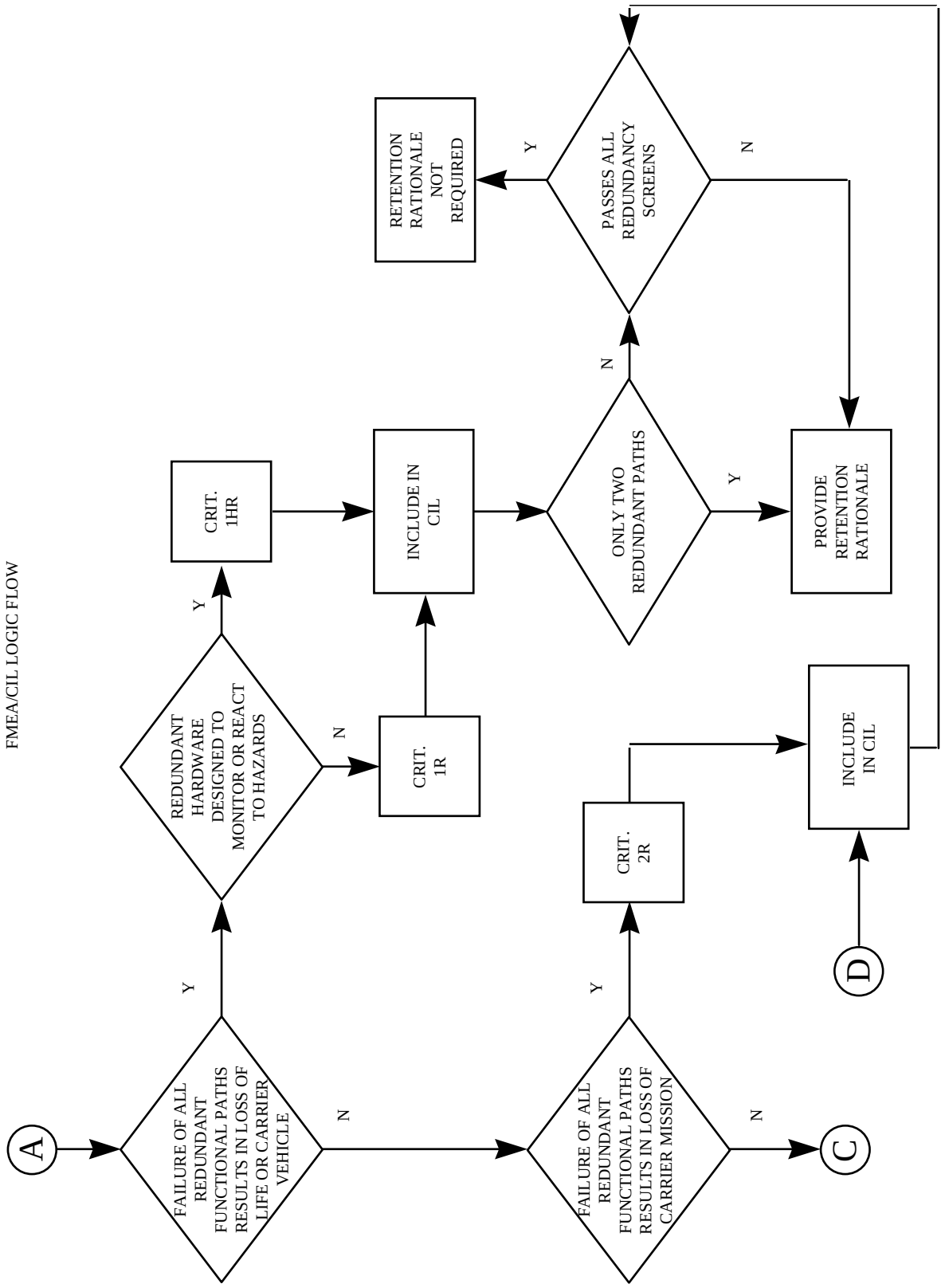
C. Criticality Category Definitions

Category	Definition
1	Single failure point resulting in loss of life or carrier vehicle.
1R	Redundant hardware elements the failure of which could cause loss of life or carrier vehicle.
1H	Single failure point rendering inoperative a system designed to monitor hazards or a system used to react to hazards; such hazards being sufficient to cause potential loss of life or carrier vehicle.
1HR	Redundant hardware elements the failure of which renders inoperative a redundant system designed to monitor hazards or react to hazards; such hazards being sufficient to cause potential loss of life or carrier vehicle.
2	Single failure point of payload/experiment hardware resulting in loss of carrier vehicle mission.
2R	Redundant hardware elements the failure of which could cause loss of carrier vehicle mission.
2P	Single failure point resulting in loss of payload/experiment hardware or loss of payload/experiment mission objectives.
2PR	Redundant hardware elements the failure of which could cause loss of hardware or mission, as specified in category 2P above.
3	All others.



FME A/CIL LOGIC FLOW

FIGURE 1



FMEA/CIL LOGIC FLOW

FIGURE 1 (CONT'D)

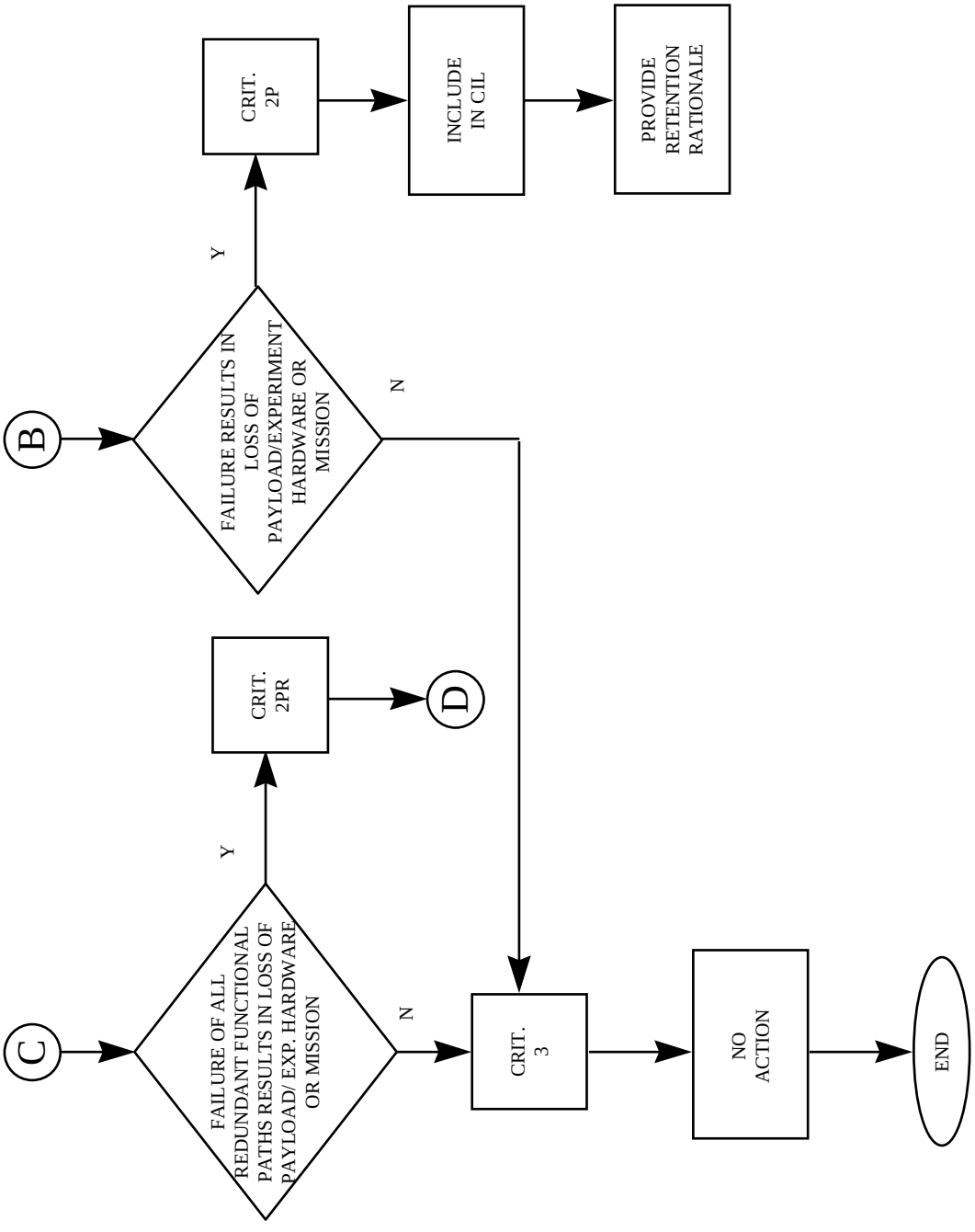


FIGURE 1 (CONT'D)

D. Failure Modes

1. All possible failure modes will be identified and analyzed for each component during each of the predetermined mission phases.

2. The analysis will assume that all inputs to the component being analyzed are present and correct.

3. The analysis will assume that only one failure mode has occurred at any given time, and this will be the basis for establishing the criticality category for individual components.

4. The analysis will include the loss of function (where redundant components are used) by assuming failure of all redundant paths/components. This will be the basis for assigning criticality categories designated by an "R" (i.e., 1R, 1HR, 2R, and 2PR) for the component members of all redundant/backup configurations. Each failure mode entry for redundant items will include notations to indicate compliance with redundancy screens defined in paragraphs II.B.1, 2, and 3.

E. Emergency Systems - Independent emergency or contingency safing systems shall not be considered as redundancy in determining the criticality category of any flight system or GSE hardware. All emergency systems or components, which are required to operate only when another system or component has failed, will be analyzed for all failure modes. Criticality designation shall be established without regard to other failures which are pre-requisite for the emergency item to be called on, i.e., assume that the inline system has failed and the emergency system must work.

F. Standby/Backup Items - Standby and backup items which may be switched on (manually or automatically) when another item fails are not considered emergency systems. These items shall be analyzed using the groundrules which apply to redundant items under paragraph I.D.

G. Failure Mode Causes - The FMEA shall identify failure mode causes for criticality categories 1, 1R, 1H, 1HR, 2, 2R, 2P, and 2PR failure modes. The causes will be identified to a sufficient level to allow inspection and test planning that will preclude or minimize the risk of failure mode occurrence.

H. Level of analysis - For criticality 1, 1H, 1R, 1HR, 2, 2R, 2P, or 2PR, the analysis shall be conducted to the indenture level necessary to identify all single failure points, but at no time shall it be higher than the component indenture level. For criticality categories 1R, 1HR, 2R, or 2PR, the analysis shall be conducted to the

level necessary to completely verify that independent redundancy exists.

I. Detection Method and Reaction Time - The analysis shall specify the probable time for the failure effect to occur. If a detection method is available, it should be specified and the response time to safely correct the failure should be noted. If a detection system is available but would not safely correct the failure in time to prevent the undesirable effect, then this should be so noted.

J. Hazard Identification - Effects of both single and multiple failures (where multiple failures refer only to those functions where redundant items are used), which can result in a hazardous condition shall be identified.

K. Hardware/Software Analysis Requirements[1]

1. The hazard/software analysis, as specified in this paragraph, shall be documented separately from the FMEA containing the hardware systems analyses.

2. Software responses to hardware failure modes and software commands to hardware shall be analyzed for all software which directly supports or controls the operation of the payload/experiment. This analysis should include the hardware/software interfaces and the human/software interface, as applicable.

3. The analysis shall identify and document all hardware failures which affect software. The analysis of failure effects on software shall identify and confirm the method of failure detection, identify and confirm the response, and confirm that the response is consistent with overall system objectives. The hardware/software analysis shall use the same failure mode coding as the hardware FMEA. (See section VI for detailed instructions.)

II. CRITICAL ITEMS LIST (CIL)

A. Critical Items List Content - Based on the results of the FMEA, a CIL shall be prepared consisting of a single failure point (SFP) summary and a summary of all critical redundant items (including backup items). The CIL shall contain all criticality category 1, 1R, 1H, 1HR, 2, 2R, 2P, and 2PR items. This information shall be recorded per instructions given in section V.

[1] This paragraph applies only to those payloads/experiments that are required by section VII. to conduct a hardware/software analysis.

1. Redundancy Screen A - The redundant items (including standby) are capable of checkout during preparations at the launch site.

B. Rationale for Retention - Rationale for retention shall be provided for criticality categories 1 and 1H, 1R or 1HR having only two redundant paths, any 1R or 1HR that fails a redundancy screen, 2, 2P, and any 2R or 2PR that fails a redundancy screen. The redundancy screens are as follows:

2. Redundancy Screen B - Loss of a redundant item is readily detectable by the flight or ground crew. (This screen is not applicable for standby items or items that are not turned on or are otherwise inactive until called upon for use.)

3. Redundancy Screen C - The redundant items are located or so situated that no single credible cause or event such as contamination or explosion can result in loss of all redundancy.

A system of control shall be established to assure that the criteria used for verifying that the critical item passes all the screens is not changed or violated without MSFC approval.

C. Rationale for Retention Content - The rationale for retention shall address the following items:

1. Design - Identify design features which minimize the probability of occurrence of the failure mode and its causes. Identify specific characteristics and controlling aspects in the design; such as, appropriate safety factors, the use of special materials, unique physical/chemical properties, critical dimensions (as appropriate), and other measurable parameters under control that precludes or minimizes the probability of occurrence of the particular failure mode/cause for which the rationale is being presented. This rationale should describe the redundancy configuration and list the number of valid paths remaining after the first failure as well as describe how the loss of each succeeding path affects the item or critical function. (See II.C.6 below.)

2. Test - Identify and describe specific testing (including checkouts) that will be accomplished which supports the premise that the critical failure mode/cause for which the CIL is written has been properly addressed. Identify the location where the last test of the item is conducted prior to launch. A brief summary shall be provided of the test and checkout requirement(s) delineated by the Operations and Maintenance Requirements and Specifications Document (OMRSD). Reference the applicable Level II OMRSD. (See II.C.6 below.)

3. Inspection - Identify the specific inspection points (including mandatory) performed by the contractor, subcontractor, and Government Agency. Also, list the critical process controls that are implemented to minimize the probability that the failure mode causes will occur in the critical item. Relate the inspection points to the failure mode cause. (See II.C.6 below.)

4. Failure History - Provide a listing of all criticality category 1, 1R, 1H, 1HR, 2, 2R, (and 2P and 2PR at discretion of the Project Manager) item failures, causes, and the corrective actions beginning with acceptance testing[2]. Verify that failure and Unsatisfactory Condition Report (UCR) data does not show any undesirable trends.

5. Operational Use - Describe operational effect of the hardware failure, actions which can be taken by the crew following the hardware failure, crew training which minimizes the effect of the hardware failure, and mission constraints which are imposed to minimize the effect of the hardware failure. Include in-flight checkout procedures performed which can detect improper operation/loss of redundancy. (See II.C.6 below.)

6. CIL Changes - For items 1, 2, 3, and 5 above, establish the necessary documentation controls to assure that any change impacting the retention rationale for risk acceptance be processed through the Project Manager's Configuration Control Board as a minimum.

D. CIL Index - The CIL shall contain a summary of critical items consisting of one-line entries. The index shall include the FMEA item code, item name, part number, criticality category, quantity (number of items in this subsystem), and pass or fail notation for either or all redundancy screens (A, B, and/or C). An asterisk by the "item name" in the CIL Index will be used to denote those items in which failures can result in a violation of the failure tolerance requirements specified in paragraph 201 of NHB 1700.7A, "Safety Policy and Requirements for Payloads Using the Space Transportation System (STS)." A total count of the number of critical items per subsystem should be tabulated.

III. GROUNDRULES

A. Use of "Worst Case" Effects - Criticality designation shall reflect "worst case" potential effect of the failure mode.

[2] Acceptance Testing is defined as: Tests to determine that a system is capable of meeting performance requirements prescribed in the purchase specification or other documents specifying what constitutes adequate performance capability for the item in question.

B. Structures - Structures are excluded from the FMEA with the exceptions listed below:

1. Flexible fluid lines/ducts, mechanical bellows, rupture discs, sliding joints, expansion joints, and their respective attach fittings.

2. Pressure vessels, as defined by NHB 1700.7A, "Safety Policy and Requirements for Payloads Using the STS."

3. Mechanical component housings which must contain vacuum pressure, or debris from fragmentation.

4. Items which have only a single mechanical barrier between oxidizer and fuel or combustible fluid.

5. All joints that are formed by welding or brazing.

6. Any items which are required to grasp and release during any mission phase.

C. Leakage - All joints, except inspectable welded or brazed joints, shall be analyzed for leakage. Analysis will consider the worst case effects of a leak, including impingement on flammable surfaces or components.

D. Electrical Cables - Each cable assembly that carries a critical function shall be analyzed to identify and document criticality categories 1, 1H, 1R, 1HR, 2, 2R, 2P, and 2PR failure effects. The analysis shall include failure modes for open circuits, shorts to ground, and complete loss of connector(s). Adjacent pins designated to carry critical signals which upon shorting could result in improper sequence of operation with critical failure effects shall be analyzed. As a general rule, pin-to-pin failure combinations are not required in the documented analysis, but only those selected critical cases as described above.

E. Ignition - Premature ignition and failure to ignite will be considered as valid failure modes for all pyrotechnic items and solid propellants. Premature ignition may be due to either a premature electrical signal or auto-ignition.

F. Common Functions - Only one item may be analyzed when the only difference is in location. Where several components perform the same functions and have the same effects, they may be listed collectively (e.g. electrical harnesses, lines/ducts, and seals).

G. Interface - At major element interfaces (i.e., carrier vehicle /payload, Spacelab/Experiment, Stage Payload, etc.), the analysis shall include the loss of inputs and outputs between the interfacing elements. Each side of the interface must evaluate the effects of the loss of signals, or erroneous signals crossing the interface.

H. Government Furnished Equipment (GFE) - Hardware supplied as GFE shall be included in the analysis. Supporting information will be furnished to the government.

I. Orifices - Blockage of orifices shall be considered a valid failure mode and/or cause.

J. Thermal Protection System (TPS)- TPS shall be analyzed for all applicable failure modes.

IV. INSTRUCTIONS FOR THE PREPARATION OF THE FAILURE MODE AND EFFECTS ANALYSIS

INTRODUCTION

An FMEA form, such as the one shown in Figure 2, shall be used for each component/item subjected to the Failure Mode and Effects Analysis. The contents of the form shall be clear and concise. Acronyms and abbreviations used must be defined within the FMEA.

INSTRUCTIONS

The following addresses the minimum required information to be contained in each block of the FMEA form.

SYSTEM - Enter the name of the payload or experiment.

SUBSYSTEM/ASSEMBLY - Enter the name of the subsystem or assembly being analyzed.

COMPONENT/EQUIPMENT - Enter the name of the component/module subjected to the FMEA and its part number.

QUANTITY - Enter the number of this type of item in the subsystem which perform the same function in the same mission phases and the

failure of which results in the same effects. (Reference paragraph III.F)

DRAWING/SCHEMATIC - Enter the component/module drawing identification number.

REFERENCE - Provide the identification number of the functional flow diagram and/or other appropriate reference material.

PREPARED BY/APPROVED BY - Identification of the analyst who performed the FMEA and individual responsible for overall FMEA effort.

PAGE/DATA/REV - Enter page number and total number of pages per component/equipment FMEA. Provide a revision number and date for each page. A notation shall be made opposite each entry that has been changed since the previous submittal (i.e., a change bar on the right of the change).

MISSION PHASE - Phase of mission in which the failure occurs. The analysis must include the following mission phases: pre-launch; ascent; on-orbit operations; contingency/return (applies to deployable payloads only; refers to return to earth without deploying payload); nominal return; and STS intact abort. The analysis shall also consider specific mission phases for each payload/experiment as required by the Project Office. More than one phase may be checked providing the information is the same for each phase checked.

FMEA ITEM CODE - Unique number assigned to the item under analysis.

FUNCTION/DESCRIPTION REFERENCE DESIGNATION - Concise statement of the function(s) performed. Provide the drawing/schematic reference designation.

FAILURE MODE/FAILURE CAUSE - Identification of the specific failure mode after considering the four basic failure conditions below:

1. Unscheduled operation
2. Failure to operate when required
3. Failure to cease operations when required
4. Failure during operation.

For each applicable hardware failure mode, list the major cause(s), including operational and environmental stress, if known (e.g., thermal, contamination, micrometeoroids, radiation, piece-part electrical short, vibration, etc.).

FAILURE EFFECTS

(a) ITEM/SYSTEM: Effects on the component, equipment, subsystem, and the interfacing subsystem.

(b) MISSION: Effects on the carrier vehicle, payload, or experiment mission objectives.

(c) HARDWARE: Effects on the payload or experiment hardware.

(d) CARRIER VEHICLE/CREW: Effects on the carrier vehicle and the flight or ground crew.

CRIT - Assign a failure mode criticality category designation in relation to crew safety and mission effect. Criticalities are: 1, 1R, 1H, 1HR, 2, 2R, 2P, 2PR, and 3.

REDUNDANCY SCREENS - Indicate pass/fail/not applicable for each of the redundancy screens shown in paragraphs II.B.1, 2, and 3.

REMARKS

(a) REDUNDANCY AND CORRECTIVE ACTION: Provide a description of alternative means of operation and/or redundancy available after a failure. Identify the corrective action, automatic or manual, to be taken in the event of the failure and identify the operational procedures written for this contingency. State the time between the failure and the failure effect.

(b) DETECTION METHOD & REACTION TIME: For each failure mode, provide the following information, as applicable (See paragraph VIII.E.16, for definitions):

- Detection Method (if any available)
- Time of Detection
- Time Available
- Time required

Reaction times are to be specified as follows:

- Immediate - Less than a second
- Seconds - 1 to 60 seconds
- Minutes - 1 to 60 minutes
- Hours - 1 to 24 hours
- Days - 1 day to mission complete

(c) SOFTWARE RESPONSE: (Applies only to those payloads/experiments which are required to conduct a hardware/software analysis; see section VII): For a hardware failure mode that impacts software, indicate the hardware/software analysis item number where the software response to the hardware failure is documented. In the hardware/software analysis, include a reference to the requirement(s) that specifies a software response to the hardware failure, if such exists.

ANALYST REMARKS - The analyst shall add any pertinent remarks or recommendations at his/her discretion. Failure modes which create a potentially hazardous situation shall be noted here.

FAILURE MODE AND EFFECTS ANALYSIS

SYSTEM:_____ MISSION PHASE:

SUBSYSTEM/ASSEMBLY:_____ ___1. PRELAUNCH

COMPONENT/EQUIPMENT:_____ ___2. ASCENT

QUANTITY:_____ ___3. DEPLOYMENT

DRAWING/SCHEMATIC:_____ ___4. OPERATIONS

REFERENCE:_____ ___5. CONTINGENCY/RETURN

PAGE___ OF___ DATE:_____

REV:_____

PREPARED BY:_____

APPROVED BY:_____

FMEA ITEM CODE	FUNCTION/DESCRIPTION REFERENCE DESIGNATOR	FAILURE MODE/ CAUSE	FAILURE EFFECTS (A) ITEM/SYSTEM (B) PAYLOAD MISSION (C) SHUTTLE VEHICLE/CREW	CRIT.	REDUNDANCY SCREENS A, B, C (P, F, N/A)	REMARKS (A) REDUNDANCY & CORR. ACTION (B) DET. METH. & REACTION TIME (C) SOFTWARE RESPONSE

FIGURE 2
Typical FMEA Worksheet

V. INSTRUCTIONS FOR THE PREPARATION OF THE CRITICAL ITEMS LIST (CIL)

INTRODUCTION

The CIL shall contain an index as specified in paragraph II. D. A separate critical item sheet shall be prepared for each unique failure mode described in the Failure Mode and Effects Analysis (FMEA) with effect(s) that are criticality categories 1, 1R, 1H, 1HR, 2, 2R, 2P, or 2PR. Those redundant (R) items that pass the three screens will be entered into the CIL, but will not require retention rationale except for "1R" or "1H" items having only two redundant paths. Any "R" item which fails a screen will require retention rationale. A system of control will be established and reported in the CIL to assure that the criteria used for verifying that the critical item passes all the screens is not changed or violated without MSFC approval. The respective controls shall be traceable to the specific causes leading to the failure mode. The CIL shall be performed using the form shown in Figure 3.

INSTRUCTIONS

The following addresses each numbered block in the CIL form as to what information is required for entry, as a minimum. Additional pages may be used, if necessary, for completeness.

BLOCK NUMBER	ENTRY INSTRUCTIONS
(1)	SYSTEM/SUBSYSTEM Enter the name of the system or subsystem being analyzed.
(2)	FUNCTION Enter the system/subsystem function per the FMEA.
(3)	FMEA ITEM CODE Enter the alpha-numeric item code assigned to the item in the FMEA and cross-referenced to the block diagram to identify the CIL entry.
(4)	REV. NO. AND DATE Enter the revision number/letter and date of revision. If there is no revision at the time of submittal, enter the date CIL was effective and leave the revision block blank.

BLOCK NUMBER	ENTRY INSTRUCTIONS

(5) ANALYST

Enter the name of the person performing the analysis for the CIL entry.

(6) APPROVED BY

Enter the name of the individual who reviews and issues approval for the CIL entry

(7) CRITICALITY CATEGORY

Enter whether the failure mode effect is criticality 1, 1R, 1H, 1HR, 2, 2R, 2P, or 2PR. This categorization shall be compatible with the criticality category of the failure mode effect described in the FMEA for the specific hardware.

(8) PART NAME

Enter the same hardware name used in the FMEA.

(9) PART NUMBER

Enter the drawing part number corresponding to the part name.

(10) PHASES

Enter the mission phase in which failure occurs: e.g., prelaunch; ascent; deployment; operations; contingency/return (abort); nominal return; intact abort.

(11) QUANTITY

Indicate the number of hardware items which: (a) have the same part name and number in the subsystem, and, (b) perform the same function, and, (c) whose failure modes and effects are identical (see paragraph III.F).

(12) EFFECTIVITY

Identify the flight configuration(s) for which the failure mode is applicable.

(13) HAZARD REF.

Enter the Hazard Analysis Reference Number when applicable. (See section VIII.)

BLOCK NUMBER — ENTRY INSTRUCTIONS

(14) FAILURE MODE AND EFFECTS

Enter the failure mode description from FMEA. Use one failure mode per sheet. Describe (in summary form) the failure effects associated specifically with the failure mode and relate the effect to the criticality category in block (7).

(15) FAILURE CAUSE(S)

A failure mode and effect may have more than one cause. Enter each contributing cause separately, since the rationale for retention will address each cause individually. Each cause (e.g., contamination, misalignment, broken wire, bearing frozen, cracked blades, piece-part failures) shall be specifically identified as a line item.

(16) REDUNDANCY SCREENS

Redundant items, including backup items, classified as criticality category 1R, 1HR, 2R, or 2PR shall be analyzed to determine whether the redundancy screens shown in II.B.1, 2, 3, are passed or failed. Criticality categories are based on FMEA results.

(17) RATIONALE FOR RETENTION - Provide information as specified in item II.C. of Groundrules.

State the justification for retaining the critical item.

Figure 3
CIL Form

CRITICAL ITEMS LIST (CIL)

(1) SYSTEM/SUBSYSTEM _____
(2) FUNCTION _____
(3) FMEA ITEM CODE _____
(4) REV. NO. & DATE _____
_____
(5) ANALYST _____
(6) APPROVED BY _____

(7) CRIT. CATEGORY _____
(8) PART NAME _____
(9) PART NO. _____
(10) PHASE(S) _____
(11) QUANTITY _____
(12) EFFECTIVITY _____
(13) HAZARD REF _____

(14) FAILURE MODE AND EFFECT:

(15) FAILURE CAUSE(S): a.

b.

(16) REDUNDANCY SCREENS:

NOTE: INDICATE PASS/FAIL AND EXPLAIN AS NECESSARY

SCREEN A _____
SCREEN B _____
SCREEN C _____

(17) RATIONALE FOR RETENTION:

[17A.] DESIGN: a.

b.

[17B.] TEST: a.

b.

[17C.] INSPECTION: a.

b.

[17D.] FAILURE HISTORY/RELATED EXPERIENCE:

a.

b.

[17E.] OPERATIONAL USE:

a.

b.

VI. INSTRUCTIONS FOR PREPARATION OF THE HARDWARE/SOFTWARE ANALYSIS

INTRODUCTION - The Hardware/Software Analysis shall contain the following information. The Hardware FMEA form shown in Figure 2, may be modified and used for this task, if desired.

SYSTEM - Enter the name of the payload/experiment.

SUBSYSTEM/SOFTWARE SEGMENT - Enter the name of the hardware subsystem and the software system and release number (i.e., DFF-224 FSW Version 5.4) under consideration.

COMPONENT/EQUIPMENT - Enter the name of the hardware component/module, the failure mode of which is being considered in the hardware/software analysis.

DESIGN REQUIREMENT - Enter the title and applicable sections of the software design requirements document.

REFERENCE - Identify any pertinent reference material.

PREPARED BY/APPROVED BY - Identification of the analyst who performed the analysis and individual responsible for overall analysis effort.

PAGE/DATE/REV - Enter the page number and total number of pages per software segment being analyzed. Provide a revision number and date for each page. A notification shall be made opposite each entry that has been changed since the previous submittal (i.e., a change bar on the right of the change).

MISSION PHASE[3] - Phase of mission in which failure occurs. More than one phase may be checked providing the information is the same for each phase checked.

FUNCTION - Concise statement of the software function performed.

FAILURE MODE[3] - Identification of the specific hardware failure mode and effects being considered for its effect on software. Reference the hardware FMEA code identifier.

CRIT[3] - The failure mode criticality category assigned to the hardware failure effects.

[3] This information should be taken directly from the hardware FMEA.

SOFTWARE COMPLIANCE - Document the software's compliance with requirements in the following areas:

(1) State the method by which the software detects the hardware failure under consideration. (out-of-limit test, redundancy management algorithm, error code, interrupt, etc.)

(2) State the software reaction time to respond to the hardware failure.

(3) Describe the software's response to the hardware failure (Error notification, hardware commands, system reconfiguration, etc.).

(4) Where applicable, correlate responses to (1) - (3) to specific Software Requirements Document paragraphs.

VII. FMEA/CIL PERFORMANCE CRITERIA

A. PAYLOAD AND EXPERIMENT CLASSIFICATION

All MSFC managed payloads/experiments using the Space Transportation System (STS) may be classified in accordance with the following classification systems unless otherwise directed:

CLASS "A"

Payloads for which a minimum risk approach is clearly dictated by prohibitively high cost of the consequences of failure, or by an unacceptable combination of costs and intangible factors associated with failure. Success critical single failure points (SFP's)[4] are not permitted except by formal project level waiver, if they can be avoided by functional or block redundancy. Retention of unavoidable SFP's requires justification based on risk analysis and implementation of measure to minimize risk.

CLASS "B"

Payloads for which an approach characterized by reasonable compromise between minimum risks and minimum costs is appropriate due to capability to recover from in-flight failure by some means that is marginally acceptable even though it involves significantly high costs and/or highly undesirable intangible factors. Success critical SFP's are permitted without a formal waiver. Single string and partially single string design approaches are acceptable.

[4] Success Critical Single Failure Points (SFP's) are those which would result in the inability of payload equipment to achieve the set of objectives, or meet the set of requirements, that compromise the criteria by which success or failure of the equipment will be judged.

CLASS "C"

Payloads for which re-flight of repeat flight[5] is planned as a routine backup in the event of in-flight "soft[6]" failure, and re-flight or repeat flight costs are low enough to justify limiting qualification and acceptance testing to end item environmental screening. There is no significant intangible or tangible impact of "soft" failure except the cost of repair and re-flight, or repeat flight, which is estimable with reasonable confidence and is directly tradeable with in-flight reliability enhancement costs. Therefore, a decision criteria of minimum total expected cost is appropriate and practical. Success critical SFP's are permitted without a formal waiver. Single string and partially single string design approaches are acceptable.

CLASS "D"

Payloads that have objectives worth achieving at a cost not to exceed the amount required for a single low cost attempt where formal verification requirements are limited to those required for safety and compatibility. Success critical SFP's are permitted without a formal waiver. Single string and partially single string design approaches are acceptable.

Individual payloads are assigned an overall classification based on the criteria above. Separate classification at lower indenture levels is also allowed (e.g., a Class A free-flyer payload may incorporate instruments from Classes A and B. A Class A Spacelab Payload may incorporate instruments from all classes.).

B. FMEA/CIL PERFORMANCE REQUIREMENTS

FMEA's shall be performed on payloads/experiments as shown below.

FMEA's are required for:

1. All class A payload/experiment hardware. A Hardware/Software analysis shall also be prepared.

[5] Any equipment failure resulting in failure of a payload to meet its success criteria, but not resulting in any safety hazard, propagation of failure to the STS, or any other payload equipment, or damage to hardware other than the failed payload.

[6] "Repeat flight " denotes the use of a new flight article to achieve the same objectives. "Re-flight" refers to the use of the same article.

2. All Class B payload/experiment hardware. A Hardware/Software analysis shall not be prepared unless specifically required by the Project Manager.

3. Analysis of Class C and Class D payload/experiment hardware is required only in those cases where a potential catastrophic or critical hazard associated with a specific functional hardware failure mode is identified by the hazard analysis. An FMEA worksheet and Critical Item Sheet is required for each hazard meeting the aforementioned criteria. The FMEA worksheet and Critical Item Sheet shall be included as an attachment to the hazard report for the payload/experiment. FMEA's for other Class C or Class D hardware shall not be prepared unless specifically required by the Project Manager.

VIII. DEFINITIONS

E.1 Component - A combination of parts, devices, and structures, usually self-contained, which perform a distinctive function in the operation of the overall equipment. Also, referred to as a "black box."

E.2 Corrective Action - An identification of actions, automatic or manual, which could be taken to circumvent the failure.

E.3 Critical Item - An item whose loss of function results in any of the following failure effects:

1. Loss of life
2. Loss of carrier vehicle
3. Loss of carrier mission objectives
4. Loss of payload/experiment hardware
5. Loss of payload/experiment mission objectives

E.4 Emergency System or Hardware - Any system or hardware item which is used only after a life threatening situation has occurred because of prior failures or events; this includes jettisonable hardware, smoke detection/fire suppression, etc. This excludes hardware which performs a function used during any nominal mission phase.

E.5 Failure - The inability of a system, subsystem, component, or part to perform its required function within specified limits, under specified conditions for a specified duration.

E.6 Failure Mode - A description of the manner in which an item can fail.

E.7 Failure Cause - Any credible event or phenomena which can generate a failure of an item.

E.8 Fail-Operational - The ability to sustain a failure and retain sufficient operational capability for safe mission continuation.
E.9 Fail-Safe - The ability to sustain a failure and retain the capability to successfully terminate the mission.

E.10 Hazard - The presence of a potential risk situation caused by an unsafe act or condition.

E.11 Hazard Analysis Reference - Gives the number of the Hazard Report associated with the critical failure mode.

E.12 Inputs - Any mechanical, thermal, electrical, electromagnetic, or optical signal/quantity/phenomena or operator action required by a component in order to operate normally.

E.13 Payload - Any equipment or material carried that is not considered part of the carrier vehicle. This includes items such as free-flying automated spacecraft, individual experiments or instruments, support equipment, etc.

E.14 Redundancy - Multiple ways of performing a function:

(A) Operational Redundancy - Redundant items, all of which are fully energized during the subsystem operating cycle. Operational redundancy includes load sharing redundancy wherein redundant items are connected in such a manner that, upon failure of one unit, the remaining items will continue to perform the subsystem function. It is not necessary to switch out the failed item or switch in the redundant item.

(B) Standby Redundancy - Redundant hardware items that are nonoperative (have no power applied) until they are switched into the subsystem upon failure of the primary item.

(C) Like Redundancy - Identical hardware items performing the same function.

(D) Unlike Redundancy - Nonidentical hardware items performing the same function.

E.15 Single Failure Point - A single item of hardware, the failure of which could lead directly to loss of life: life or carrier vehicle (criticality category 1); system for monitoring or reacting to hazards or hazardous conditions (criticality category 1H); carrier mission objectives (criticality category 2); payload/experiment hardware or mission objectives (criticality category 2P).

E.16 Reaction Time - The time from failure occurrence to failure effect. This time includes the following elements:

Time of Detection - The time period from the time of the failure until the time the failure is detected. This time is unavailable since corrective action cannot be initiated until detection.

Time Available - The usable period of reaction time. This is the period from the time of detection until the last point in time prior to failure effect during which the failure can be counteracted.

Time Required - The response time required to safely correct the failure. This time period is from the time of the detection until the corrective action is completed. This time frame includes the time to initiate corrective action.